CSCI 1515 Applied Cryptography

This Lecture:

- ZKP for OR Statements (Continued)
- Anonymous Online Voting (Continued)
- ElGamal Threshold Encryption
- RSA Blind Signature

Anonymous Online Voting

Public: Cyclic group G of order q with generator g

ElGamal public key pk

Exponential ElGamal

ZKP

Voter 1 $\longrightarrow$ $Enc(v_1) = (g^{r_1}, pk^{r_1} \cdot g^{v_1})$ $v_1 \in \{0, 1\}$

Voter 2 $\longrightarrow$ $Enc(v_2) = (g^{r_2}, pk^{r_2} \cdot g^{v_2})$ $v_2 \in \{0, 1\}$

$\vdots$

Voter n $\longrightarrow$ $Enc(v_n) = (g^{r_n}, pk^{r_n} \cdot g^{v_n})$ $v_n \in \{0, 1\}$

$\Downarrow$

$Enc(\Sigma v_i) = (g^{\Sigma r_i}, pk^{\Sigma r_i} \cdot g^{\Sigma v_i})$

$\Downarrow$

Decrypt to Σv_i

Correctness of Encryption

Given a cyclic group G of order q with generator g. (public)

Public key $pk \in G$. ← public

Ciphertext $C = (c_1, c_2)$ ← public

ZKP for an OR statement:

C is an encryption of 0 OR C is an encryption of 1

Witness: randomness r used in encryption

↑ secret

$$R_L = \{ ((pk, c_1, c_2), r) : (c_1 = g^r \wedge c_2 = pk^r) \vee (c_1 = g^r \wedge c_2 = pk^r \cdot g) \}$$

↑ (public) statement ↑ (secret) witness

Correctness of Encryption

$R_L = \{ ((h,u,v), b) \text{ s.t. } u = g^b \wedge v = h^b \}$

(h,u,v): public, b: secret

C is an encryption of 0

Witness: randomness r used in encryption

$R_{L_0} = \{ ((pk, c_1, c_2), r) : c_1 = g^r \wedge c_2 = pk^r \}$

(pk, c1, c2): (public) statement; r: (secret) witness

C is an encryption of 1

Witness: randomness r used in encryption

$R_{L_1} = \{ ((pk, c_1, c_2), r) : c_1 = g^r \wedge \cancel{c_2 = pk^r \cdot g} \}$

$c_2 \cdot g^{-1}$

$c_2 \cdot g^{-1} = pk^r$

(pk, c1, c2): (public) statement; r: (secret) witness

Proving AND/OR Statements

AND: Statements: x_0, x_1

Witnesses: w_0, w_1

$$R_{AND} = \{ ((x_0, x_1), (w_0, w_1)) : (x_0, w_0) \in R_{L_0} \text{ AND } (x_1, w_1) \in R_{L_1} \}$$

OR: Statements: x_0, x_1

Witness: w

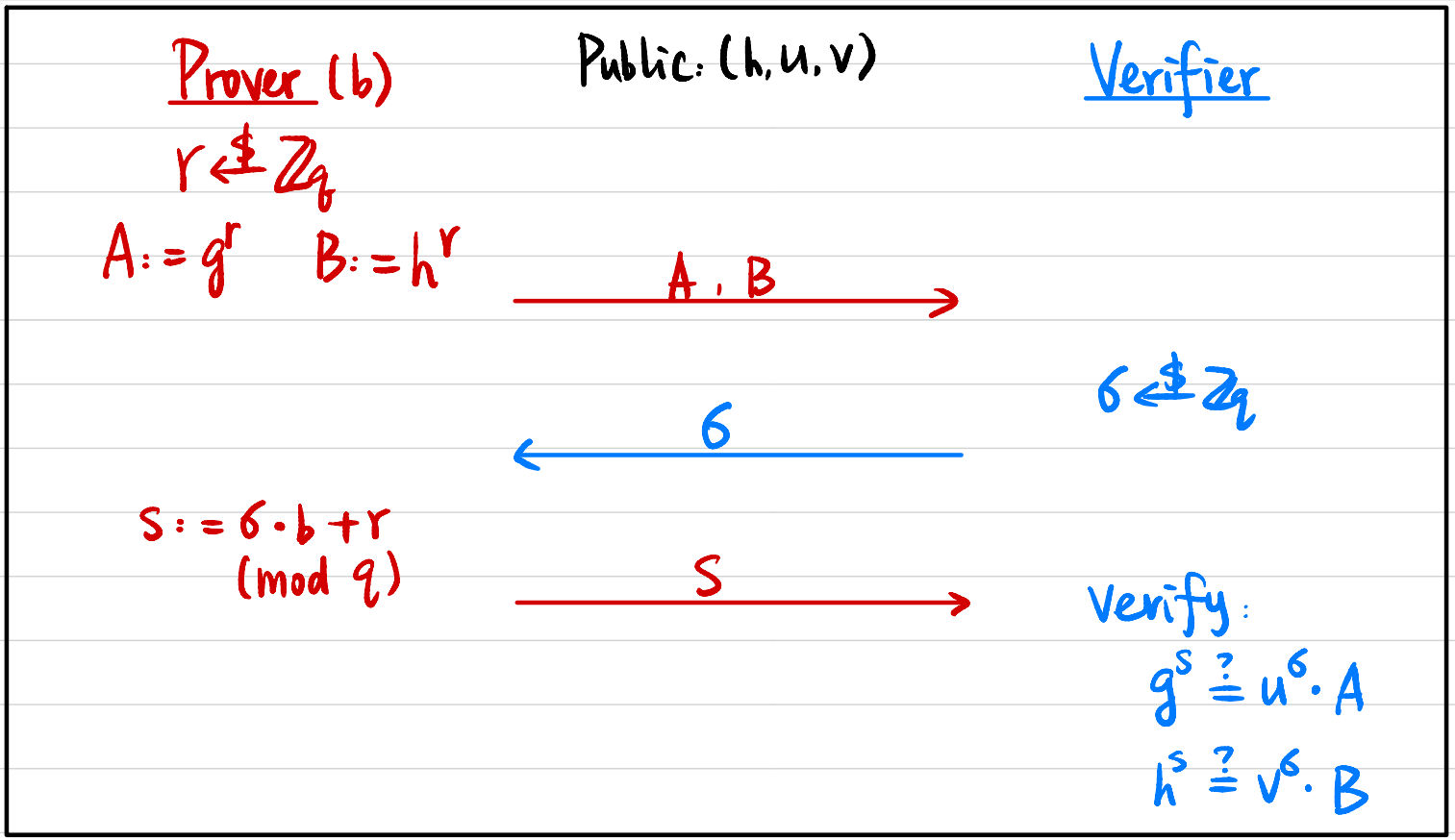
$$R_{OR} = \{ ((x_0, x_1), w) : (x_0, w) \in R_{L_0} \text{ OR } (x_1, w) \in R_{L_1} \}$$

Example: Diffie-Hellman Tuple

Public: Cyclic group G of order q, generator g, $(h,u,v) = (g^a, g^b, g^{ab}) = (z, g^b, z^b)$

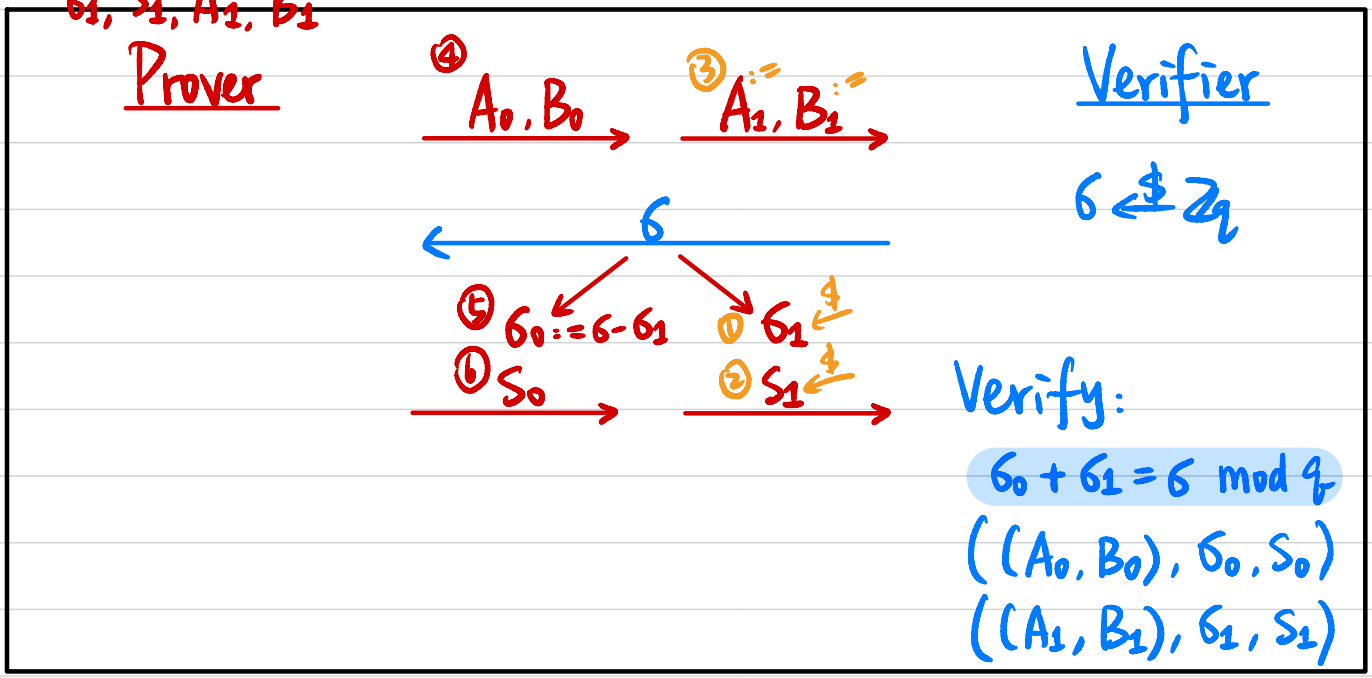
Prover's secret witness: b s.t. $u = g^b \wedge v = h^b$

$R_L = \{ ((h,u,v), b) \}$



Proving OR Statement

$$R_{OR} = \{ ((x_0, x_1), w) : (x_0, w) \in R_{L_0} \text{ OR } (x_1, w) \in R_{L_1} \}$$



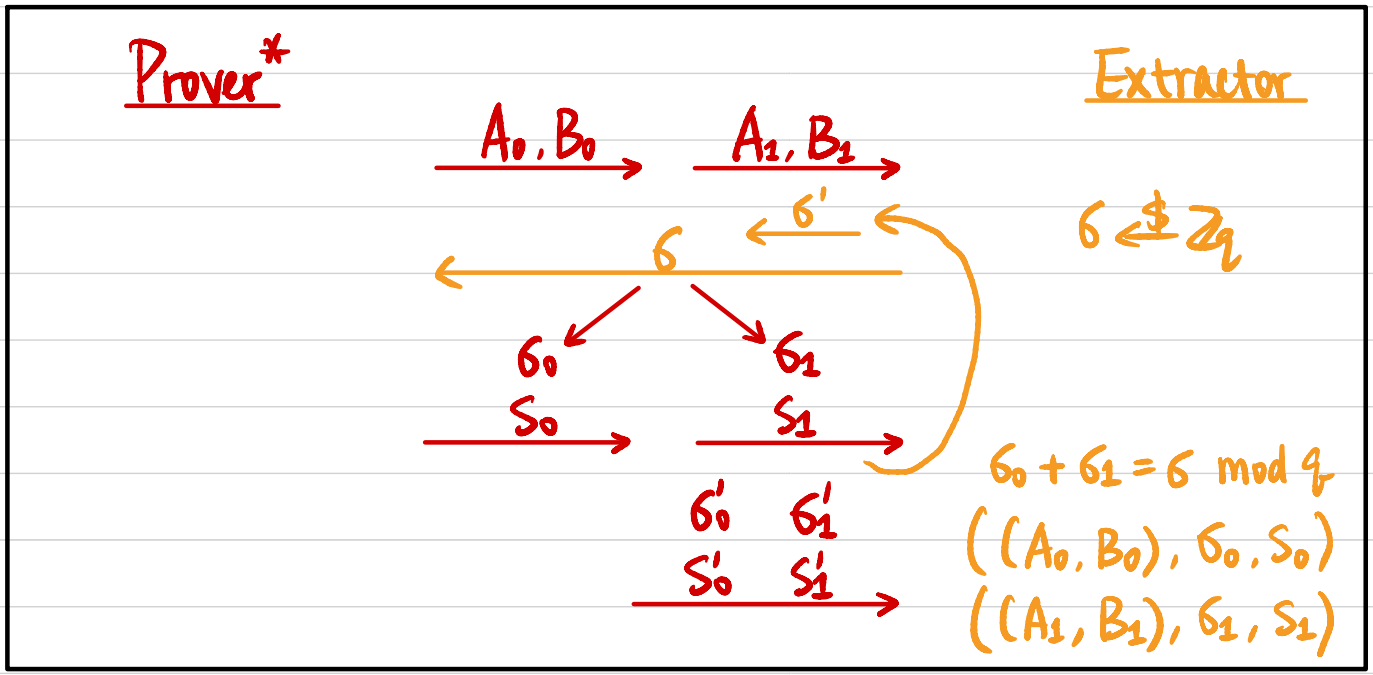
How does Prover compute response for both statements?

Say $(x_0, w_0) \in R_{L_0}$

Completeness? Completeness + HVZK of underlying ZKP

Proving OR Statement

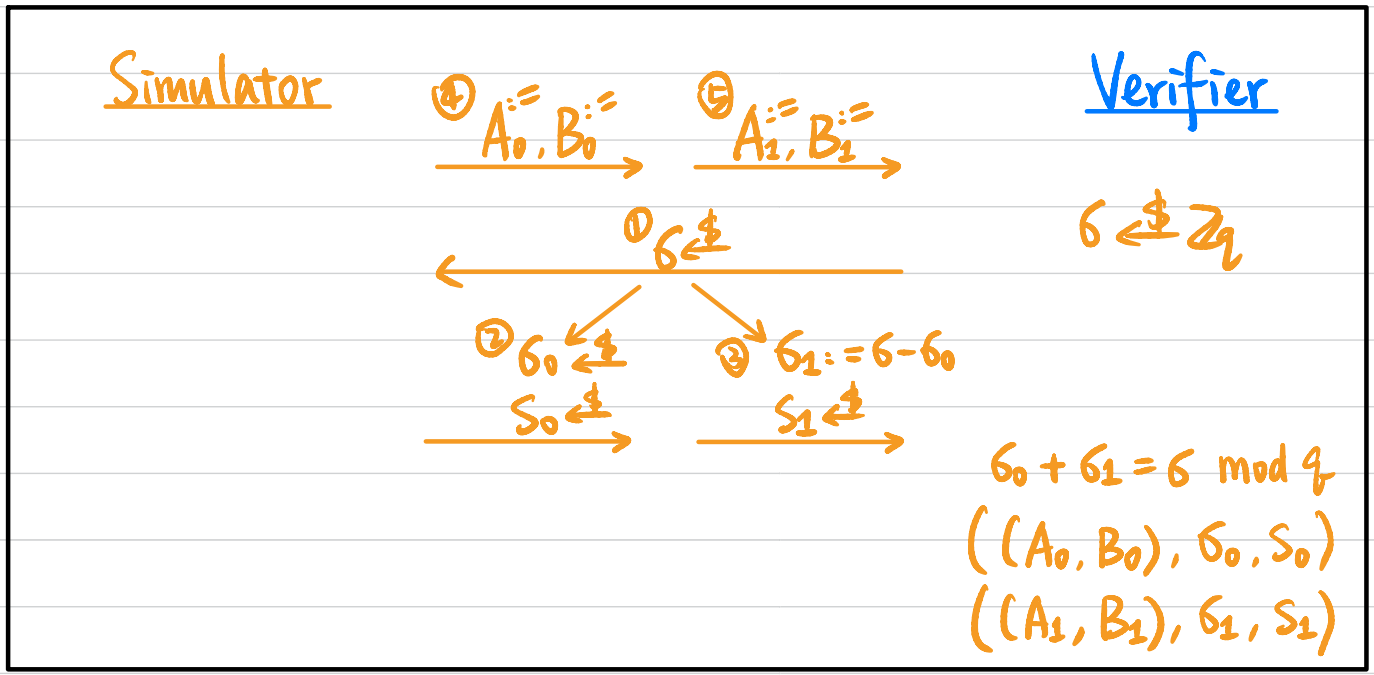
Proof of Knowledge?



How to extract w s.t. $(x_0, w) \in R_{L_0}$ OR $(x_1, w) \in R_{L_1}$?

Proving OR Statement

Honest-Verifier Zero-Knowledge (HVZK)?



Anonymous Online Voting

Public: Cyclic group G of order q with generator g

ElGamal public key pk $(= g^{sk})$

Exponential ElGamal

ZKP

Voter 1 $\longrightarrow$ $Enc(v_1) = (g^{r_1}, pk^{r_1} \cdot g^{v_1})$ $v_1 \in \{0, 1\}$

Voter 2 $\longrightarrow$ $Enc(v_2) = (g^{r_2}, pk^{r_2} \cdot g^{v_2})$ $v_2 \in \{0, 1\}$

$\vdots$

Voter n $\longrightarrow$ $Enc(v_n) = (g^{r_n}, pk^{r_n} \cdot g^{v_n})$ $v_n \in \{0, 1\}$

$\Downarrow$

$Enc(\Sigma v_i) = (g^{\Sigma r_i}, pk^{\Sigma r_i} \cdot g^{\Sigma v_i}) = (C_1, C_2)$

$\Downarrow$

Decrypt to Σv_i

How? Who?

$\Downarrow$

$C_2 / C_1^{sk} = g^{\Sigma v_i}$

$\{g^0, g^1, \cdots, g^n\}$

Threshold Encryption

t-out-of-t threshold

P_1: $(pk_1, sk_1) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_1$

P_2: $(pk_2, sk_2) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_2$

$\vdots$

P_t: $(pk_t, sk_t) \leftarrow \text{PartialGen}(1^\lambda) \longrightarrow pk_t$

$\Rightarrow pk$

$ct \leftarrow \text{Enc}_{pk}(m)$

P_1: $d_1 \leftarrow \text{PartialDec}(sk_1, ct) \longrightarrow d_1$

P_2: $d_2 \leftarrow \text{PartialDec}(sk_2, ct) \longrightarrow d_2$

$\vdots$

P_t: $d_t \leftarrow \text{PartialDec}(sk_t, ct) \longrightarrow d_t$

$\Rightarrow m$

Threshold Encryption: ElGamal

P_1: $sk_1 \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_1 = g^{sk_1}$ $\longrightarrow$ pk_1

P_2: $sk_2 \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_2 = g^{sk_2}$ $\longrightarrow$ pk_2

$\vdots$

P_t: $sk_t \xleftarrow{\$} \mathbb{Z}_q$ $\quad pk_t = g^{sk_t}$ $\longrightarrow$ pk_t

$\Rightarrow pk = \prod pk_i = \prod g^{sk_i} = g^{\sum sk_i}$

$sk = \sum sk_i \bmod q$

$ct = (c_1, c_2) = (g^r,\ pk^r \cdot g^m)$

P_1: $d_1 = c_1^{sk_1}$ $\longrightarrow$ d_1

P_2: $d_2 = c_1^{sk_2}$ $\longrightarrow$ d_2

$\vdots$

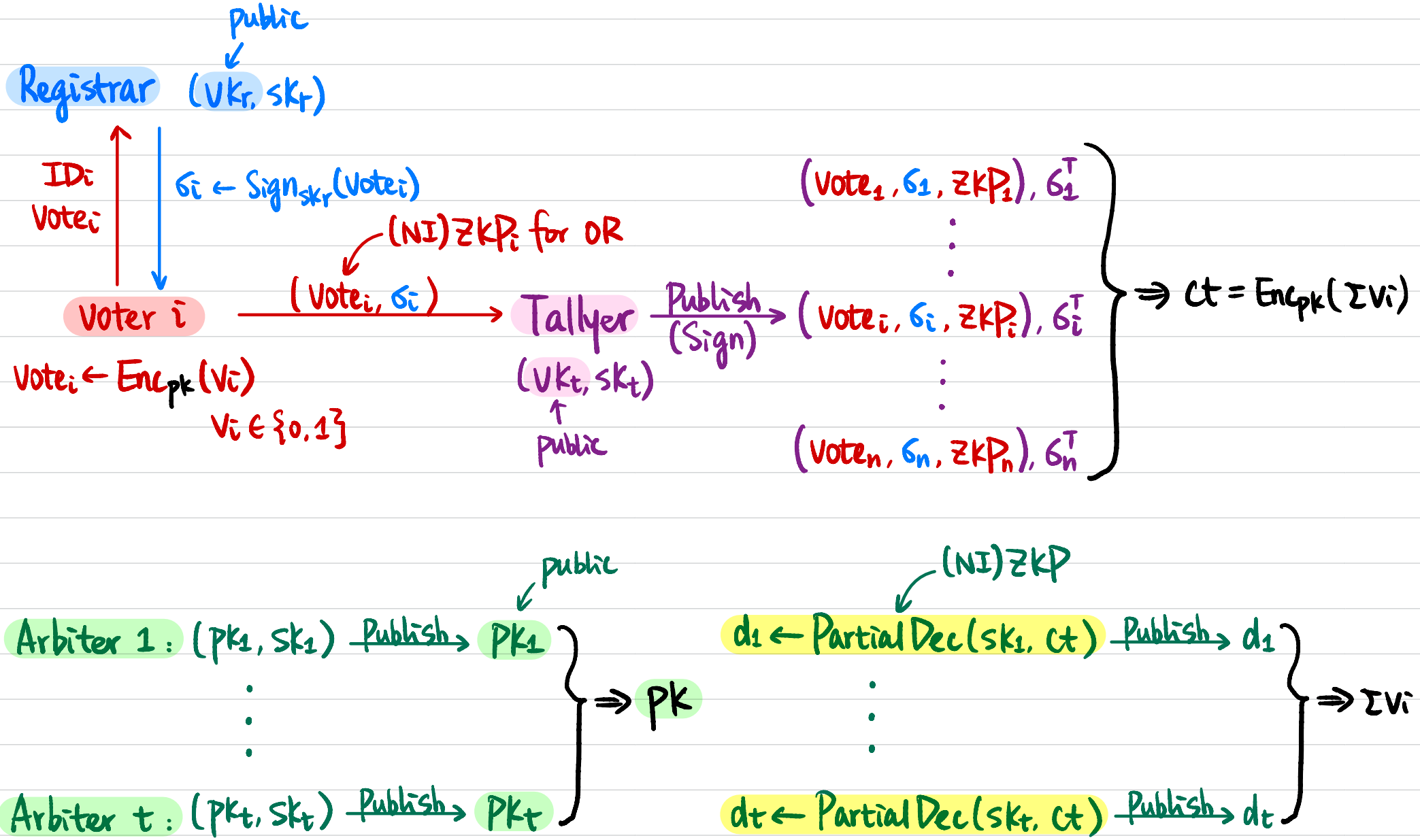
P_t: $d_t = c_1^{sk_t}$ $\longrightarrow$ d_t

$\Rightarrow \prod d_i = c_1^{\sum sk_i} = c_1^{sk}$

$m = ?$

$c_2 / c_1^{sk} \rightarrow g^m \rightarrow m$

Anonymous Online Voting



Correctness of Partial Decryption

Given a cyclic group G of order q with generator g. (public)

Partial public key $pk_i \in G$.

Ciphertext $C = (C_1, C_2)$. ← public

Partial decryption d_i

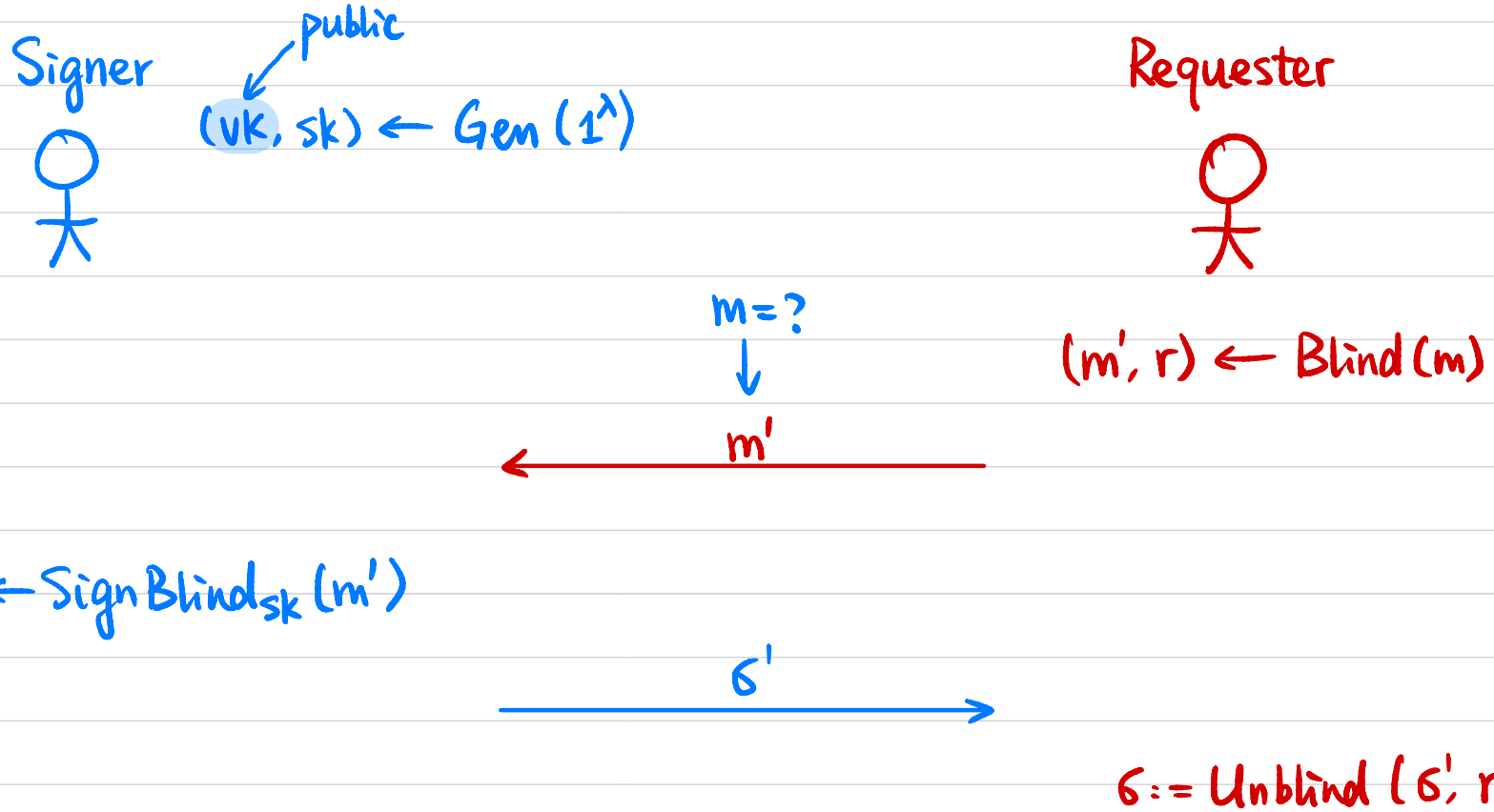
Witness: partial secret key sk_i ← private

ZKP for partial decryption:

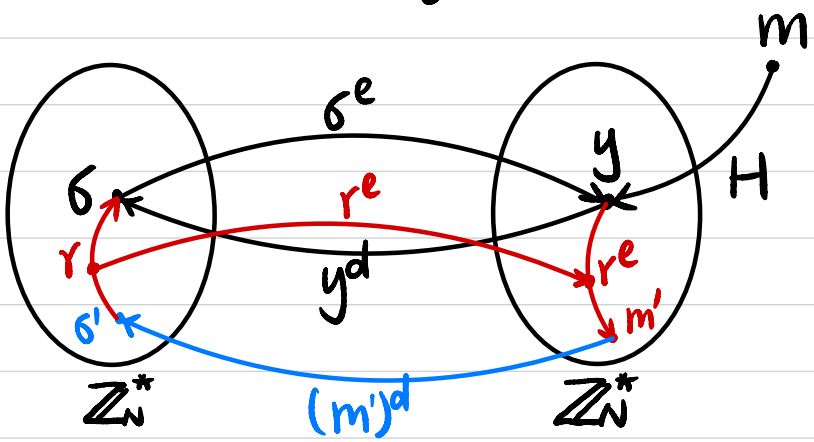
$$R_L = \{ (\underbrace{(C_1, pk_i, d_i)}_{\text{public}}, \underbrace{sk_i}_{\text{secret}}) : \quad pk_i = g^{sk_i} \wedge d_i = C_1^{sk_i} \}$$

$$R_L = \{ (\underbrace{(h, u, v)}_{\text{public}}, \underbrace{b}_{\text{secret}}) \text{ s.t. } u = g^b \wedge v = h^b \}$$

Blind Signature



RSA Blind Signature



$VK = (N, e)$ $\quad$ $Sk = d$

$Sign_{sk}(m) = H(m)^d \bmod N$

$Vrfy_{VK}(m, \sigma)$: $\sigma^e \stackrel{?}{\equiv} H(m) \pmod N$

Signer

$(VK, sk) \leftarrow Gen(1^\lambda)$

$m = ?$

$\downarrow$

m' $\longleftarrow$

$SignBlind_{sk}(m')$:

$\sigma' := (m')^d$

σ' $\longrightarrow$

Requester

$Blind(m)$:

$r \xleftarrow{\$} \mathbb{Z}_N^*$

$m' := H(m) \cdot r^e \bmod N$

$Unblind(\sigma', r)$:

$\sigma := \sigma' \cdot r^{-1} \bmod N$

$\sigma^e = (\sigma')^e \cdot (r^{-1})^e = (m')^{d \cdot e} \cdot r^{-e} = m' \cdot r^{-e}$

$= H(m) \cdot r^e \cdot r^{-e} = H(m)$